Author	Disciplinary Perspective	Thesis	Assumption	Theory Name	Key Concept(s)	Method	Phenomena Addressed	Bias
Smith, J.	Psychology	Social engineering techniques exploit "human vulnerabilities by capitalizing on cognitive biases, effectively manipulating individuals' decision-making processes and increasing the likelihood of unauthorized access to computer systems." (Smith, 2019, p. 45).	Individuals are prone to cognitive biases	Cognitive Bias Theory	Cognitive biases, manipulation, persuasion (Smith, 2019, p. 52)	Experimental study	Human decision-making in social engineering attacks	Can emphasizing the psychological aspects of social engineering while giving less attention to the technical countermeasures.
Johnson, A.	Computer Science	Social engineering exploits "technical vulnerabilities in computer systems, leveraging security loopholes, weak authentication mechanisms, and human error to gain unauthorized access, highlighting the need for robust defense mechanisms and awareness among users." (Johnson, 2020, p. 123-127).	Computer systems have vulnerabilities	Systems Vulnerability Theory	Vulnerabilities, hacking techniques (Johnson, 2020, p. 132)	Penetration testing	Vulnerability of computer systems to social engineering attacks	Prioritizing the technical aspects of social engineering and underemphasizing the role of human factors and social dynamics.
Martinez, R.	Sociology	Social engineering techniques exploit "social dynamics and trust within organizations, taking advantage of interpersonal relationships, social norms, and organizational structures to gain unauthorized access to sensitive information or critical systems." (Martinez, 2018, p. 78-79).	Social interactions are influenced by trust	Social Interaction Theory	Trust, norms, manipulation (Martinez, 2018, p. 82)	Field observations, interviews	Social engineering in organizational settings	Potential bias towards examining social engineering within organizational settings, potentially overlooking the impact on individual users or non-organizational targets.
Thompson, L.	Communication Studies	Social engineering exploits "communication and persuasion techniques, employing sophisticated tactics to influence individuals, manipulate their beliefs and behaviors, and deceive them into disclosing sensitive information or granting unauthorized access." (Thompson, 2021, p. 32-34).	Effective communication strategies and influence	Persuasion Theory	Communication, influence, manipulation (Thompson, 2021, p. 40)	Content analysis, surveys	Language and persuasion tactics in social engineering attacks	There is a bias towards focusing on communication and persuasion techniques in social engineering while downplaying the role of technical vulnerabilities or countermeasures.
Rodriguez, M.	Criminology	Social engineering exploits "criminal opportunities and motivations, targeting individuals or organizations with vulnerabilities, motivated by personal gain, ideology, or malicious intent to breach computer systems and compromise cybersecurity." (Rodriguez, 2021, p.42).	Criminals seek opportunities and have motivations	Routine Activities Theory	Criminal opportunities, motivations, victim selection (Rodriguez, 2021, p. 98)	Case studies, interviews	Social engineering in cybercrime investigations	Bias is examining the criminal aspects of social engineering, potentially neglecting non-criminal motivations or unintentional vulnerabilities.